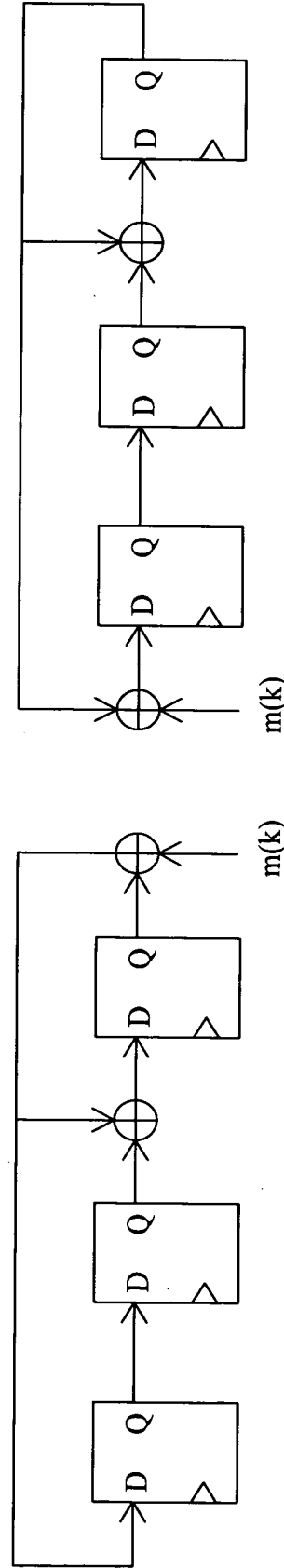


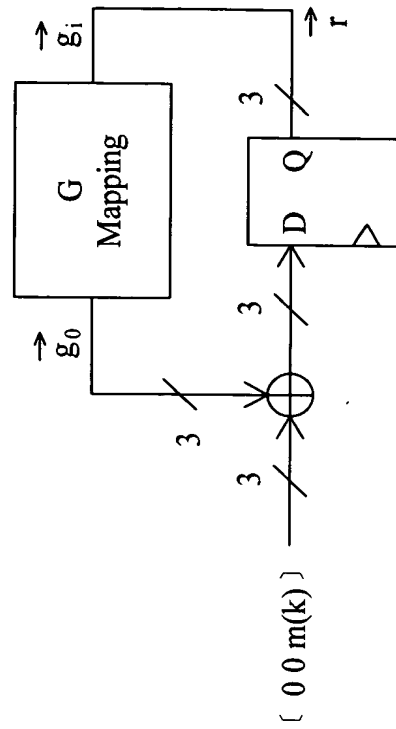
$$g(x) = x^3 + x^2 + 1$$



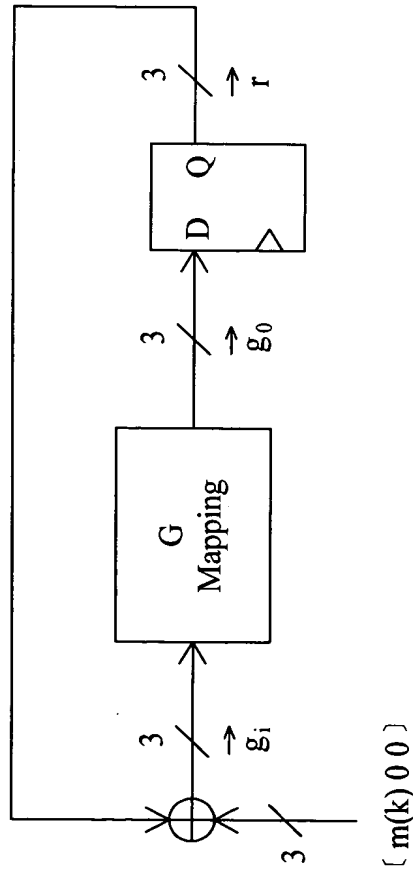
Scheme 1

Scheme 2

Fig. 1



Scheme 2



Scheme 1

Fig. 2

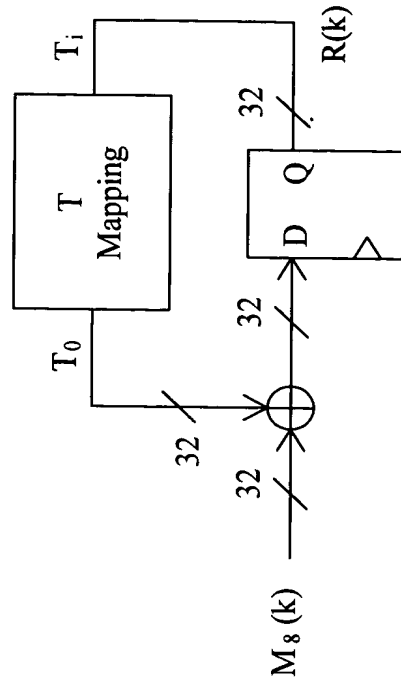
G =

Row31	0x40000000
Row30	0x20000000
Row29	0x10000000
Row28	0x08000000
Row27	0x04000000
Row26	0x82000000
Row25	0x01000000
Row24	0x00800000
Row23	0x80400000
Row22	0x80200000
Row21	0x00100000
Row20	0x00080000
Row19	0x00040000
Row18	0x00020000
Row17	0x00010000
Row16	0x80008000
Row15	0x00004000
Row14	0x00002000
Row13	0x00001000
Row12	0x80000800
Row11	0x80000400
Row10	0x80000200
Row9	0x00000100
Row8	0x80000080
Row7	0x80000040
Row6	0x00000020
Row5	0x80000010
Row4	0x80000008
Row3	0x00000004
Row2	0x80000002
Row1	0x80000001
Row0	0x80000000

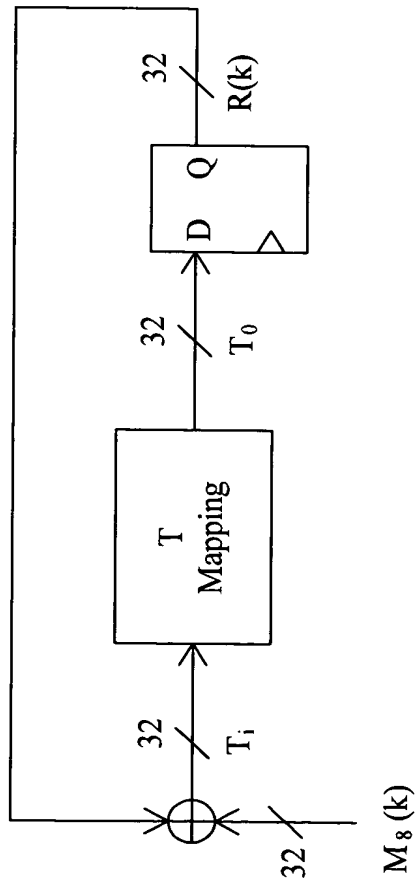
G<sup>-1</sup> =

Row31	0x00000001
Row30	0x80000000
Row29	0x40000000
Row28	0x20000000
Row27	0x10000000
Row26	0x08000000
Row25	0x04000001
Row24	0x02000000
Row23	0x01000000
Row22	0x00800001
Row21	0x00400001
Row20	0x00200000
Row19	0x00100000
Row18	0x00080000
Row17	0x00040000
Row16	0x00020000
Row15	0x00010001
Row14	0x00008000
Row13	0x00004000
Row12	0x00002000
Row11	0x00001001
Row10	0x00000801
Row9	0x00000401
Row8	0x00000200
Row7	0x00000101
Row6	0x00000081
Row5	0x00000040
Row4	0x00000021
Row3	0x00000011
Row2	0x00000008
Row1	0x00000005
Row0	0x00000003

Fig. 3



Scheme 2



Scheme 1

Fig. 4

$T = G^8 =$

Row31	0x20800000	2
Row30	0x90400000	3
Row29	0xc8200000	4
Row28	0x64100000	4
Row27	0xb2080000	5
Row26	0x59040000	5
Row25	0x0c020000	3
Row24	0x86010000	4
Row23	0x43008000	4
Row22	0x01004000	2
Row21	0x20002000	2
Row20	0x10001000	2
Row19	0x88000800	3
Row18	0xc4000400	4
Row17	0x62000200	4
Row16	0x31000100	4
Row15	0xb8000080	5
Row14	0xdc000040	6
Row13	0xee000020	7
Row12	0x77000010	7
Row11	0x1b000008	5
Row10	0x2d000004	5
Row9	0x36000002	5
Row8	0x1b000001	5
Row7	0xad000000	5
Row6	0xf6000000	6
Row5	0xfb000000	7
Row4	0x5d000000	5
Row3	0x8e000000	4
Row2	0xc7000000	5
Row1	0xc3000000	4
Row0	0x41000000	2

$T^{-1} = G^{-8} =$

Row31	0x000000d5	5
Row30	0x0000006a	4
Row29	0x00000035	4
Row28	0x0000001a	3
Row27	0x0000000d	3
Row26	0x00000006	2
Row25	0x000000d6	5
Row24	0x0000006b	5
Row23	0x80000035	5
Row22	0x400000cf	7
Row21	0x200000b2	5
Row20	0x10000059	5
Row19	0x0800002c	4
Row18	0x04000016	4
Row17	0x0200000b	4
Row16	0x01000005	3
Row15	0x008000d7	7
Row14	0x0040006b	6
Row13	0x00200035	5
Row12	0x0010001a	4
Row11	0x000800d8	5
Row10	0x000400b9	6
Row9	0x00040089	4
Row8	0x00020044	3
Row7	0x000080f7	8
Row6	0x000040ae	6
Row5	0x00002057	6
Row4	0x000010fe	8
Row3	0x000008aa	5
Row2	0x00000455	5
Row1	0x000002ff	9
Row0	0x000001aa	5

Fig. 5

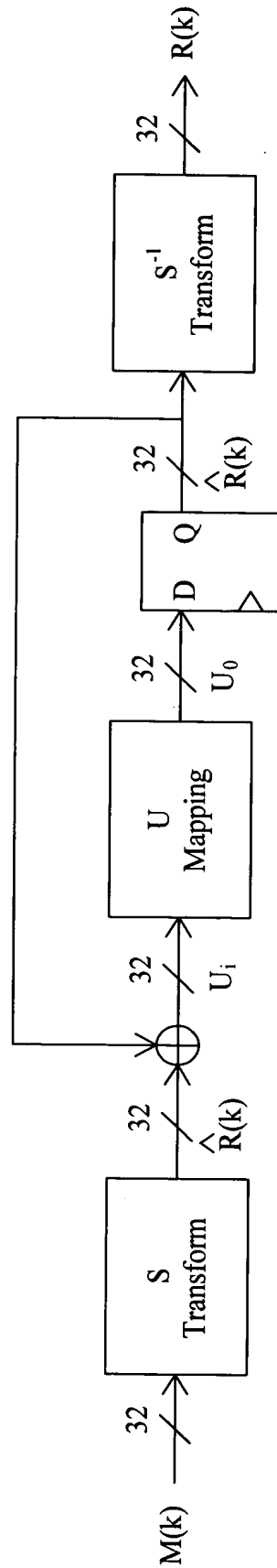


Fig. 6

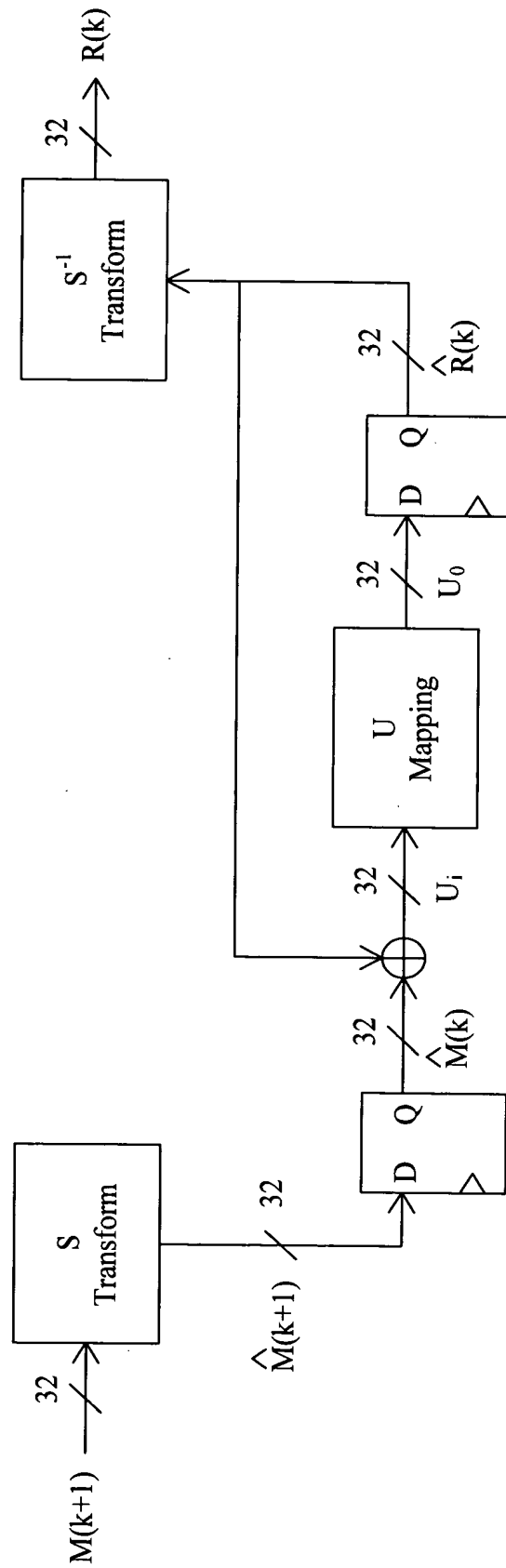


Fig. 7

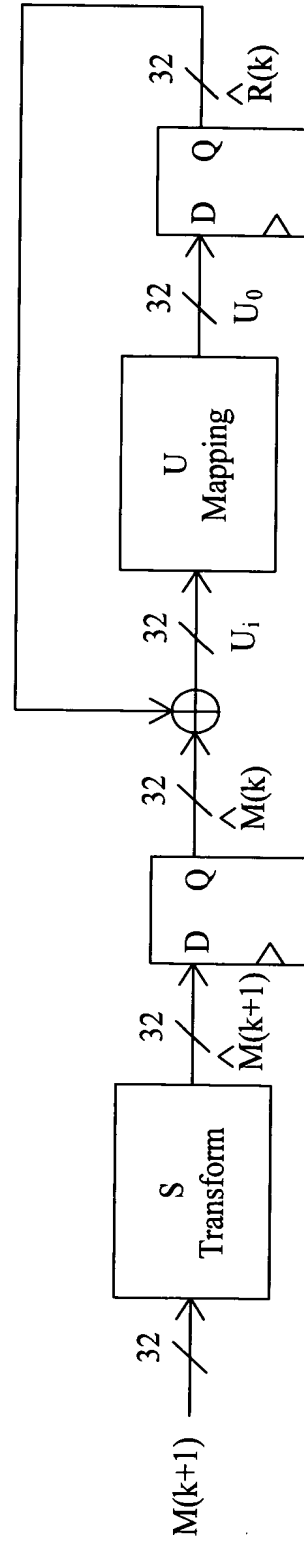


Fig. 8



$$U_{32} =$$

Row31	0xfb808a20	12
Row30	0x7dc04590	13
Row29	0xbec022c8	14
Row28	0x5e70116d	15
Row27	0x2fb809b2	15
Row26	0x97dc0459	15
Row25	0xb06e8804	11
Row24	0x5837448e	14
Row23	0xac1ba243	14
Row22	0xac8d5b00	13
Row21	0xad462620	12
Row20	0x57a31311	14
Row19	0x2b518888	11
Row18	0x95a8c4cc	14
Row17	0xcad46262	14
Row16	0x646a3130	12
Row15	0x483593b9	15
Row14	0x249ac8d4	13
Row13	0x924d64e6	15
Row12	0x6610e0b0	11
Row11	0x0fd1ce00	13
Row10	0xb4096225	12
Row9	0x20843b3f	14
Row8	0x91c21c1a	12
Row7	0x33e185a5	15
Row6	0x627048fe	15
Row5	0x313824fb	15
Row4	0xe21c9854	13
Row3	0x8a0ec786	15
Row2	0x4f09a449	13
Row1	0x18033bc2	12
Row0	0xf6011640	11

Fig. 9

$S_{32} = S_{32}^{-1} =$

Row31	0x80000000	1
Row30	0x40000000	1
Row29	0x20000000	1
Row28	0x10000000	1
Row27	0x08000000	1
Row26	0x04000000	1
Row25	0x02000000	1
Row24	0x01000000	1
Row23	0x00800000	1
Row22	0x00400000	1
Row21	0x00200000	1
Row20	0x00100000	1
Row19	0x00080000	1
Row18	0x00040000	1
Row17	0x00020000	1
Row16	0x00010000	1
Row15	0x00008000	1
Row14	0x00004000	1
Row13	0x00002000	1
Row12	0x01001001	3
Row11	0x00000900	2
Row10	0x00000400	1
Row9	0x00000200	1
Row8	0x00000100	1
Row7	0x00000080	1
Row6	0x00000040	1
Row5	0x00000020	1
Row4	0x00000010	1
Row3	0x00000008	1
Row2	0x0000000c	2
Row1	0x00000002	1
Row0	0x00000001	1

Fig. 10

$U_{tx\_08} =$

Row31	0x20800000	2
Row30	0x90400000	3
Row29	0xc8200000	4
Row28	0x64100000	4
Row27	0xb2080000	5
Row26	0x59040000	5
Row25	0x0c020000	3
Row24	0x86010000	4
Row23	0x03008000	3
Row22	0x21004000	3
Row21	0x00002000	1
Row20	0x00001100	2
Row19	0x88000900	4
Row18	0xc4000400	4
Row17	0x62000200	4
Row16	0x31000100	4
Row15	0x28000080	3
Row14	0x04200040	3
Row13	0x22200020	4
Row12	0x08100010	3
Row11	0x00000009	2
Row10	0x2c000004	4
Row9	0x36000002	5
Row8	0x1b000001	5
Row7	0x8c004000	4
Row6	0x92100000	4
Row5	0xa2040000	4
Row4	0x1c000000	3
Row3	0x8e000000	4
Row2	0x41010000	3
Row1	0xc3000000	4
Row0	0x41000000	2

Fig. 11

$$S_{tx\_08} = S_{tx\_08}^{-1} =$$

Row31	0x80000000	1
Row30	0x40000000	1
Row29	0x20000000	1
Row28	0x10000000	1
Row27	0x08000000	1
Row26	0x04000000	1
Row25	0x02000000	1
Row24	0x01000000	1
Row23	0x00800000	1
Row22	0x00400000	1
Row21	0x00200000	1
Row20	0x00100000	1
Row19	0x00080000	1
Row18	0x00040000	1
Row17	0x00020000	1
Row16	0x00010000	1
Row15	0x40008000	2
Row14	0x20004000	2
Row13	0x20002000	2
Row12	0x10001100	3
Row11	0x00000900	2
Row10	0x00000400	1
Row9	0x00000200	1
Row8	0x00000100	1
Row7	0x00400080	2
Row6	0x10000040	2
Row5	0x04000020	2
Row4	0x00000011	2
Row3	0x00000008	1
Row2	0x01000004	2
Row1	0x00000002	1
Row0	0x00000001	1

Fig. 12

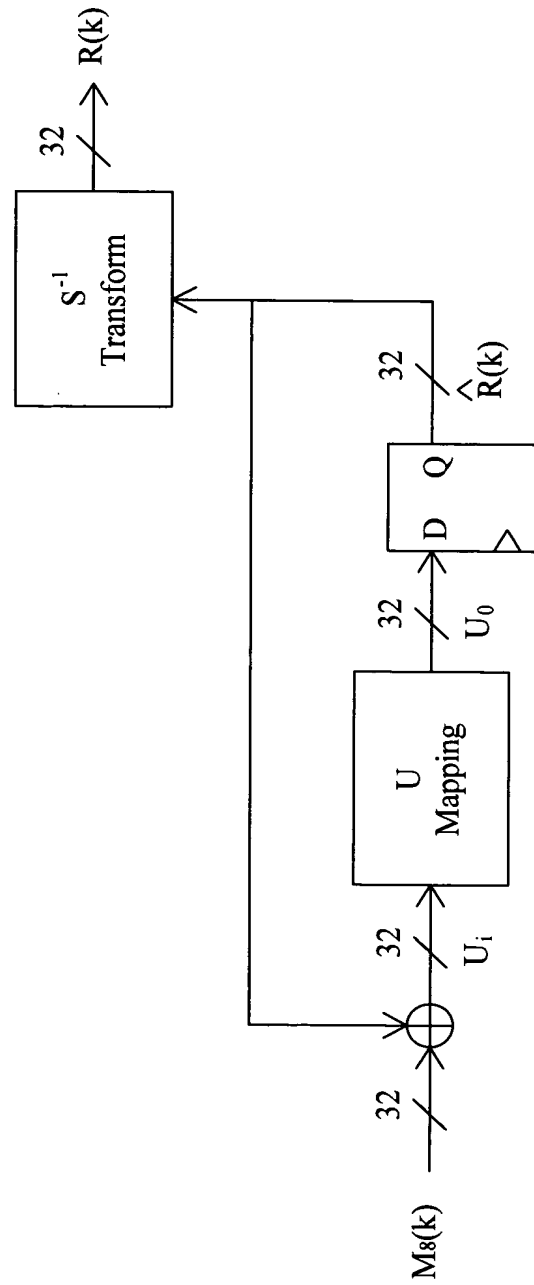


Fig. 13

$U_{rx\_08} =$

Row31	0x20800000	2
Row30	0x90400000	3
Row29	0xc8200000	4
Row28	0x64100000	4
Row27	0xb2080000	5
Row26	0x59040000	5
Row25	0x0c020000	3
Row24	0x86010000	4
Row23	0x03008000	3
Row22	0x21004000	3
Row21	0x00022000	2
Row20	0x00001040	2
Row19	0x88000900	4
Row18	0xc4000400	4
Row17	0x62000200	4
Row16	0x31000100	4
Row15	0x28000080	3
Row14	0x04200040	3
Row13	0x00200030	3
Row12	0x08500010	4
Row11	0x00000009	2
Row10	0x2c000004	4
Row9	0x36000002	5
Row8	0x1b000001	5
Row7	0x8c004000	4
Row6	0x92100000	4
Row5	0x00400002	2
Row4	0x04040000	2
Row3	0x8e000000	4
Row2	0x41010000	3
Row1	0xc3000000	4
Row0	0x41000000	2

Fig. 14

$S_{rx\_08} =$	Row31	0x80000000	1
	Row30	0x40000000	1
	Row29	0x20000000	1
	Row28	0x10000000	1
	Row27	0x08000000	1
	Row26	0x04000000	1
	Row25	0x02000000	1
	Row24	0x01000000	1
	Row23	0x00800000	1
	Row22	0x00400000	1
	Row21	0x00200000	1
	Row20	0x00100000	1
	Row19	0x00080000	1
	Row18	0x00040000	1
	Row17	0x00020000	1
	Row16	0x00010000	1
	Row15	0x40008000	2
	Row14	0x20004000	2
	Row13	0x20022000	3
	Row12	0x00001040	2
	Row11	0x00000900	2
	Row10	0x00000400	1
	Row9	0x00000200	1
	Row8	0x00000100	1
	Row7	0x00400080	2
	Row6	0x10000040	2
	Row5	0x40000230	4
	Row4	0x04000010	2
	Row3	0x00000008	1
	Row2	0x01000004	2
	Row1	0x00000002	1
	Row0	0x00000001	1

$S_{rx\_08}^{-1} =$	Row31	0x80000000	1
	Row30	0x40000000	1
	Row29	0x20000000	1
	Row28	0x10000000	1
	Row27	0x08000000	1
	Row26	0x04000000	1
	Row25	0x02000000	1
	Row24	0x01000000	1
	Row23	0x00800000	1
	Row22	0x00400000	1
	Row21	0x00200000	1
	Row20	0x00100000	1
	Row19	0x00080000	1
	Row18	0x00040000	1
	Row17	0x00020000	1
	Row16	0x00010000	1
	Row15	0x40008000	2
	Row14	0x20004000	2
	Row13	0x20022000	3
	Row12	0x10001040	3
	Row11	0x00000900	2
	Row10	0x00000400	1
	Row9	0x00000200	1
	Row8	0x00000100	1
	Row7	0x00400080	2
	Row6	0x10000040	2
	Row5	0x44000230	5
	Row4	0x04000010	2
	Row3	0x00000008	1
	Row2	0x01000004	2
	Row1	0x00000002	1
	Row0	0x00000001	1

Fig. 15

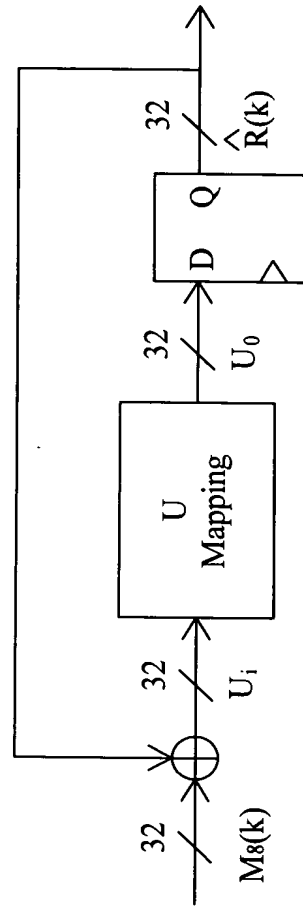


Fig. 16